

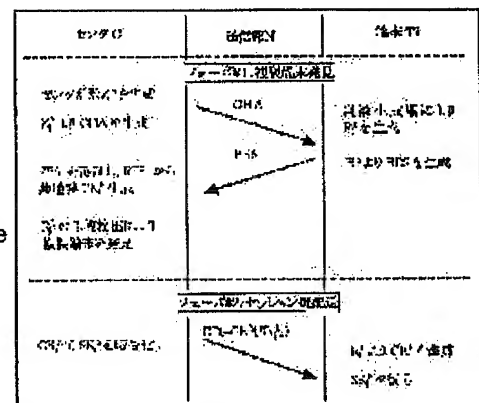
(11)Publication number : 2002-217888
(43)Date of publication of application : 02.08.2002

H04L	9/08
G06F	12/14
G06F	15/00
G09C	1/00

(71)Applicant : **ADVANCED MOBILE
TELECOMMUNICATIONS SECURITY
TECHNOLOGY RESEARCH LAB CO LTD**

(72)Inventor : ANZAI JUN
MATSUZAKI NATSUME
MATSUMOTO TSUTOMU

SOLUTION: The center and a plurality of the terminal are connected through a communication network for ciphering communication with individual session keys. The center sends challenge information in the case of delivering a new session key to the terminals. Each of the terminals sends response information obtained by ciphering terminal ID and a terminal random number to a center public key to the center, which retrieves a communication log and inspects the presence/absence of terminals, having the same terminal ID and different terminal random numbers. If corresponding terminals exist, it decides that the replicated terminal exists, and the session key will not be delivered. Since random number generated by an original terminal is difficult to replicate, the replicated terminals cannot generate the same random number. Thus, the existence of the replicated terminal can be detected.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-217888

(P2002-217888A)

(43) 公開日 平成14年8月2日 (2002.8.2)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード(参考)
H 0 4 L 9/08		G 0 6 F 12/14	3 2 0 B 5 B 0 1 7
G 0 6 F 12/14	3 2 0	15/00	3 3 0 C 5 B 0 8 5
15/00	3 3 0	G 0 9 C 1/00	6 4 0 B 5 J 1 0 4
G 0 9 C 1/00	6 4 0	H 0 4 L 9/00	6 0 1 B
			6 0 1 E

審査請求 有 請求項の数18 O L (全 16 頁)

(21) 出願番号 特願2001-11089(P2001-11089)

(22) 出願日 平成13年1月19日 (2001.1.19)

(71) 出願人 597174182

株式会社高度移動通信セキュリティ技術研究所

神奈川県横浜市港北区新横浜三丁目20番地8

(72) 発明者 安齋 潤

神奈川県横浜市港北区新横浜三丁目20番地8号 株式会社高度移動通信セキュリティ技術研究所内

(74) 代理人 100099254

弁理士 役 昌明 (外1名)

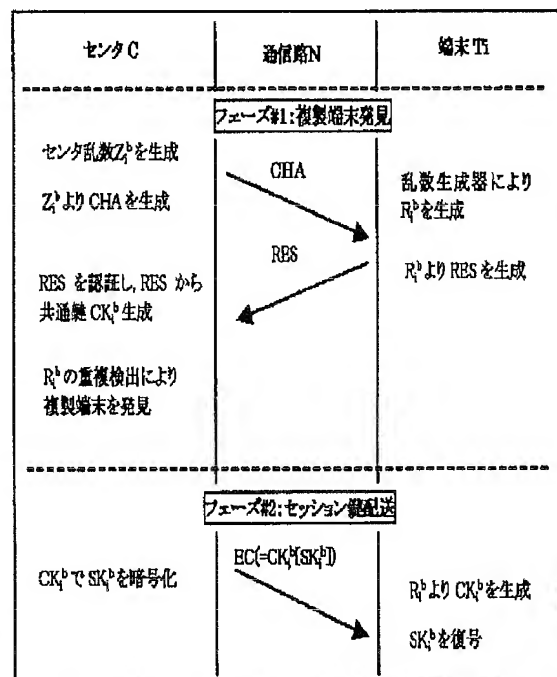
最終頁に続く

(54) 【発明の名称】 複製端末発見方法

(57) 【要約】

【課題】 センタと複数台の端末からなる通信システムにおいて、複製端末を自動的に発見して排除する。

【解決手段】 センタと複数台の端末は、個々のセッション鍵で暗号通信する通信網により接続されている。センタは、端末に新規セッション鍵を配布する際に、チャレンジ情報を送る。端末は、端末IDと端末乱数をセンタ公開鍵で暗号化したレスポンス情報をセンタに送る。センタは、通信ログを検索して、同一端末IDで端末乱数の異なる端末の有無を検査する。該当する端末があれば、複製端末が存在すると判断して、セッション鍵を配布しない。オリジナル端末で発生した乱数は複製困難であり、複製端末は同じ乱数を発生できないので、複製端末の存在を検出できる。



【特許請求の範囲】

【請求項1】 センタCとn台（nは自然数）の端末T_i（iは端末ID）を含む通信システムの複製端末発見方法において、

前記端末T_iは、ラウンドbにおける端末乱数R_b（上付きbはラウンド番号を示す添字）を生成し、前記端末乱数R_bに対する端末認証文D_bを端末秘密鍵S_iにより生成し、前記端末認証文D_bと前記端末乱数R_bとをセンタ公開鍵Y_cで暗号化して端末暗号文E_bとして前記センタCに送信し、

前記センタCは、センタ秘密鍵S_cで前記端末暗号文E_bを復号して前記端末認証文D_bと前記端末乱数R_bとを得て、端末公開鍵Y_i（センタが端末秘密鍵を管理している場合は端末秘密鍵S_i）で前記端末認証文D_bを検証し、ラウンドごとに、秘密情報の配送に使用した前記端末乱数R_bと、前記端末T_iの端末IDとを、対応させて登録したデータベースを検索して、同一端末IDでかつ異なる端末乱数が登録されている重複登録の有無を検査し、前記端末認証文D_bの検証結果が正しく、かつ前記重複登録が無い前記端末T_iの前記端末乱数R_bと前記端末IDを前記データベースに登録し、この端末乱数R_bを用いて、前記共通鍵CK_bを生成し、前記共通鍵CK_bにより秘密情報K_bを暗号化してセンタ暗号文E_cとして前記端末T_iに送信し、

前記端末T_iは、前記センタ暗号文E_cを受信し、前記端末乱数R_bから共通鍵CK_bを生成し、前記センタ暗号文E_cを前記共通鍵CK_bにより復号して前記秘密情報K_bを得ることを特徴とする複製端末発見方法。

【請求項2】 センタCとn台（nは自然数）の端末T_i（iは端末ID）を含む通信システムの複製端末発見方法において、

前記端末T_iは、ラウンドbにおける端末乱数R_b（上付きbはラウンド番号を示す添字）を生成する端末乱数生成手段と、前記端末乱数R_bに対する端末認証文D_bを端末秘密鍵S_iにより生成する認証文生成手段と、前記端末認証文D_bと前記端末乱数R_bをセンタ公開鍵Y_cで暗号化して端末暗号文E_bを生成する公開鍵暗号化手段と、前記端末暗号文E_bを送信する端末側送信手段と、前記端末乱数R_bから共通鍵CK_bを生成する端末側共通鍵生成手段と、秘密情報K_bを前記共通鍵CK_bにより暗号化したセンタ暗号文E_cを前記共通鍵CK_bにより復号化する共通鍵暗号復号手段とを備え、

前記センタCは、センタ秘密鍵S_cで前記端末暗号文E_bを復号して前記端末認証文D_bと前記端末乱数R_bを得る公開鍵暗号復号手段と、前記端末認証文D_bを端末公開鍵Y_i（センタが端末秘密鍵を管理している場合は端末秘密鍵S_i）で検証する認証文検証手段と、ラウンドごとに、秘密情報の配送に使用した前記端末乱数R_bと前記端末T_iの端末IDとを対応させて登録するデータベース手段と、前記データベースを検索して同一端末

IDでかつ異なる端末乱数が登録されている重複登録を検出する検出手段と、前記端末認証文D_bの検証結果が正しく、かつ前記重複登録が無い前記端末T_iの前記端末乱数R_bを用いて前記共通鍵CK_bを生成するセンタ側共通鍵生成手段と、前記共通鍵CK_bにより秘密情報K_bを暗号化した前記センタ暗号文E_cを生成する共通鍵暗号化手段と、前記センタ暗号文E_cを前記端末T_iに送信する送信手段とを備えたことを特徴とする複製端末発見方式。

【請求項3】 前記認証文生成手段および前記認証文検証手段を、デジタル署名を用いる手段としたことを特徴とする請求項2記載の複製端末発見方式。

【請求項4】 前記認証文生成手段および前記認証文検証手段を、鍵付きハッシュまたは共通鍵暗号を用いたメッセージ認証符号（MAC）を用いる手段としたことを特徴とする請求項2記載の複製端末発見方式。

【請求項5】 前記センタ側共通鍵生成手段および前記端末側共通鍵生成手段を、前記端末乱数R_bをそのまま前記共通鍵CK_bとして出力する手段としたことを特徴とする請求項2記載の複製端末発見方式。

【請求項6】 前記公開鍵暗号化手段と前記公開鍵暗号復号手段に代えて、Diffie-Hellman鍵共有法を含む乱数を用いた鍵共有法の1つを用いて鍵を共有する手段と、共有した鍵を改めて端末乱数として用いる手段とを設けたことを特徴とする請求項2記載の複製端末発見方式。

【請求項7】 前記センタCに、前記センタ暗号文E_cにメッセージ認証符号（MAC）を含める手段を設け、前記端末T_iに、改ざんや成りすましを検出する手段を設けたことを特徴とする請求項2記載の複製端末発見方式。

【請求項8】 前記センタCに、前記センタ暗号文E_cにデジタル署名を含める手段を設け、前記端末T_iに、改ざんや成りすましを検出する手段を設けたことを特徴とする請求項2記載の複製端末発見方式。

【請求項9】 前記秘密情報K_bが、前記センタCと前記端末T_iのセッション鍵SK_bであることを特徴とする請求項2記載の複製端末発見方式。

【請求項10】 前記秘密情報K_bを、前記センタCと複数の端末で共有されるグループ鍵GK_bとしたことを特徴とする請求項2記載の複製端末発見方式。

【請求項11】 前記端末T_iは、前記センタCから受信したセンタ乱数Z_bと前記端末乱数R_bに対する端末認証文D_bを端末秘密鍵S_iにより生成する認証文生成手段を備え、前記センタCは、前記センタ乱数Z_bを生成するセンタ乱数生成手段と、前回ラウンドにおける秘密情報の更新通知と前記センタ乱数Z_bを前記端末T_iに送信するセンタ側送信手段とを備えたことを特徴とする請求項2記載の複製端末発見方式。

【請求項12】 前記センタ乱数Z_bを、複数の端末に

共通のセンタ乱数 Z^b としたことを特徴とする請求項2記載の複製端末発見方式。

【請求項13】 前記端末 T_i に、同一ラウンドにおいて前記秘密情報が複数種類存在する場合に前記端末暗号文 E_i^b に所望の秘密情報の種類を指定する手段と、同一ラウンドにおいては常に同じ前記端末乱数 R_i^b を前記端末暗号文 E_i^b に使用する手段とを設け、前記センタ C に、同一ラウンドにおいて同一の前記端末乱数 R_i^b が使用された前記端末暗号文 E_i^b において指定された種類の秘密情報を、前記端末乱数 R_i^b より生成した前記共通鍵 CK_i^b により暗号化して配送する手段を設けたことを特徴とする請求項2記載の複製端末発見方式。

【請求項14】 前記端末 T_i に、前記センタ C からの通信を受信できない場合に前記センタ C に対して現在のラウンド番号を問い合わせる問い合わせ手段と、前記端末 T_i と前記センタ C の前記ラウンド番号 b が異なる場合に前記センタ C に再送を要求する再送要求手段とを設けたことを特徴とする請求項2記載の複製端末発見方式。

【請求項15】 前記通信システムが、同報通信システムであることを特徴とする請求項2記載の複製端末発見方式。

【請求項16】 前記センタ公開鍵 Y_c と前記センタ秘密鍵 S_c と前記端末公開鍵 Y_i と前記端末秘密鍵 S_i とを生成する手段と、前記センタ公開鍵 Y_c を全端末に配布する手段と、前記センタ秘密鍵 S_c とすべての前記端末公開鍵 Y_i とを前記センタ C に配布する手段と、前記端末秘密鍵 S_i を対応する前記端末 T_i に配布する手段とを有する信頼できるシステム管理手段を前記通信システムに備えたことを特徴とする請求項2記載の複製端末発見方式。

【請求項17】 前記端末乱数生成手段は、同じ乱数を出力する乱数生成器を他に作成できず、かつ偶然他の乱数生成器の出力と同じ出力となる確率が無視できる出力長を持つという条件を満たすことを特徴とする請求項2記載の複製端末発見方式。

【請求項18】 前記グループ鍵 GK^b の配布の途中において、複製端末が発見された場合、前記グループ鍵 GK^b を未配布の端末 T_i の端末公開鍵 Y_i （センタが端末秘密鍵を管理している場合は端末秘密鍵 S_i ）により前記グループ鍵 GK^b を暗号化して前記未配布の端末 T_i に配布する手段を備えたことを特徴とする請求項10記載の複製端末発見方式。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、複製端末発見方法に関し、特に、センタと複数の端末からなる通信システムにおける複製端末の存在を自動的に発見する複製端末発見方法に関する。

【0002】

【従来の技術】センタと複数の端末からなる通信システムにおいて、情報の秘匿や端末の認証を行なう方法として、以下のような方法がある。すなわち、センタは、セッション鍵で端末に暗号化通信を行なう。端末は、予め格納された個別の秘密鍵を用いてセッション鍵を生成または入手して、センタからの暗号通信を復号する。センタは、端末の秘密鍵で作成された認証情報を検査して端末認証を行なう。

【0003】このような方法では、秘密鍵をいかに安全に端末に格納するかが問題となる。そこで、不正なアクセスを物理的に困難にする耐タンパー性を備えた耐タンパーデバイスに、秘密鍵を格納することが多く行なわれている。一般的に、耐タンパーデバイスとしてICカードが用いられる。ICカードに端末固有の秘密鍵を保持し、端末にこのICカードを挿入して使用する方式が、GSM方式の携帯電話や有料衛星放送のSTBなどに実装されている。

【0004】しかしながら、近年はICカードに対する攻撃の研究が進み、ICカードの消費電流などから内部の秘密鍵を解読するPower Analysis Attacksなどが考案されており、ICカードの安全性は充分ではない。秘密鍵が漏洩した場合は、秘密鍵を用いた複製端末の偽造が可能になる。複製端末による暗号通信の傍受を防ぐために、暗号通信を中止して、複製端末を排除するなどの対策を講じなくてはならない。

【0005】複製端末を発見する方法としては、暗号通信の内容が外部に漏れていることから推測する方法や、ブラックマーケットにおいて複製端末を定期的に調査するといった方法があった。このような方法は、発見の確実性が低く、発見までの時間もかかるうえ、人手によらず自動的に行なうことが困難である。

【0006】これに対処するために、複製端末を事前に検出する方法が、文献1【松下達之、渡邊祐治、古原和邦、今井秀樹、“ITSに適したコンテンツ配信における不正加入者の事前検出法,” 2000年暗号と情報セキュリティシンポジウム, SCIS2000-C09, 2000.】で提案されている。

【0007】

【発明が解決しようとする課題】しかし、上記従来の事前検出法では、同報通信網とElGamal暗号と秘密分散法を前提としており、前提条件が多くて汎用性が低い。秘密分散法を利用して秘密鍵を作成すると、結託しきい値が存在することになり、結託に対して安全でない。センタが信頼できるものであっても、通信量と演算量が減らない。同一ラウンドにおいて、1端末あたり複数の秘密情報を扱うことができない。未受信対策が無い。乱数の条件が不明で安全性が不十分である。データベースが大きい。このように、システムの構成条件や動作手順が不十分で、不正端末を自動的に効率的に完全に排除することは困難であるという問題がある。

【0008】本発明は、上記従来の問題を解決して、複製端末を効率的に発見して排除することを目的とする。

【0009】

【課題を解決するための手段】上記の課題を解決するために、本発明では、センタと n 台(n は自然数)の端末を含む通信システムの複製端末発見方法を、端末は、ラウンドごとに端末乱数を生成し、端末乱数に対する端末認証文を端末秘密鍵により生成し、端末認証文と端末乱数とをセンタ公開鍵で暗号化して端末暗号文としてセンタに送信し、センタは、センタ秘密鍵で端末暗号文を復号して端末認証文と端末乱数とを得て、端末公開鍵(センタが端末秘密鍵を管理している場合は端末秘密鍵)で端末認証文を検証し、ラウンドごとに、秘密情報の配送に使用した端末乱数と、端末の端末IDとを、対応させて登録したデータベースを検索して、同一端末IDでかつ異なる端末乱数が登録されている重複登録の有無を検査し、端末認証文の検証結果が正しく、かつ重複登録が無い端末の端末乱数と端末IDをデータベースに登録し、この端末乱数を用いて、共通鍵を生成し、共通鍵により秘密情報を暗号化してセンタ暗号文として端末に送信し、端末は、センタ暗号文を受信し、端末乱数から共通鍵を生成し、センタ暗号文を共通鍵により復号して秘密情報を得る構成とした。

【0010】このように構成したことにより、端末はラウンドごとの秘密情報を入手するために、端末乱数に対する認証文を自身の秘密鍵により生成し、端末乱数と認証文をセンタの公開鍵により暗号化してセンタに送信しなければならないので、センタは同一ラウンドにおいて同じ端末秘密鍵をもつ端末から異なる端末乱数が送られてきた場合に複製端末の存在を発見できる。発見を恐れて複製端末が端末乱数を送らない場合には、複製端末は秘密情報を入手できないので、無効化することができる。同報通信網とElGamal暗号と秘密分散法を前提とせず、前提条件が少ないため、汎用性(さまざまなシステムへの適用性)が高く、適用できるシステムが多い。結託しきい値がなく、任意に作成した秘密鍵を使用することができるので、結託に対して安全である。

【0011】また、データベース手段を、ラウンドごとに、秘密情報の配送に使用した端末乱数と端末IDとを対応させて登録するデータベース手段とした。このような構成にしたことにより、データベースのサイズを小さくできる。

【0012】また、認証文生成手段および認証文検証手段を、デジタル署名方式とした。このような構成にしたことにより、センタは、各端末の秘密鍵を直接管理する必要がなく、管理が容易となり、かつセンタの不正による端末の陥れを防ぐことができる。

【0013】また、認証文生成手段および認証文検証手段を、鍵付きハッシュまたは共通鍵暗号を用いたメッセージ認証符号(MAC)方式とした。このような構成にし

たことにより、センタは認証文の検証を高速に行うことができる。センタが信頼できるという前提があれば、端末とその乱数の認証にMACを利用できるので、通信量と演算量を最小限に抑えられる。

【0014】また、共通鍵生成手段を、端末乱数をそのまま共通鍵として出力する手段とした。このような構成にしたことにより、共通鍵を容易に生成できる。

【0015】また、公開鍵暗号化手段および公開鍵暗号復号手段の代わりに、乱数を用いた鍵共有法(例えばDiffie-Hellman鍵共有法)を用いて共有した鍵を乱数として用いる構成とした。このような構成にしたことにより、端末とセンタが平等に乱数を生成することができる。

【0016】また、センタ暗号文にMACを含ませて改ざんや成りすましを検出する構成とした。このような構成にしたことにより、改ざんや成りすましを高速に検出できる。

【0017】また、センタ暗号文にデジタル署名を含ませて改ざんや成りすましを検出する構成とした。このような構成にしたことにより、センタは各端末の秘密鍵を管理することなく改ざんや成りすましを検出できる。

【0018】また、秘密情報を、センタと端末のセッション鍵とする構成とした。このような構成にしたことにより、センタと各端末の間において一時的な暗号通信や認証に利用できるセッション鍵を共有できる。

【0019】また、秘密情報を、センタと複数の端末で共有されるグループ鍵とする構成とした。このような構成にしたことにより、センタと各端末の暗号化同報通信に利用できるグループ鍵を共有できる。

【0020】また、センタの送信情報としてセンタ乱数を追加し、前記センタ乱数に対して端末が認証文を生成し、センタは前記認証文を検証することにより、認証方式がチャレンジレスポンス認証となり安全性を向上できる。

【0021】また、センタ乱数を、複数の端末に共通のセンタ乱数とした。このような構成にしたことにより、端末総数だけ必要であったセンタ乱数が1つで済む。

【0022】また、1ラウンドにおいて秘密情報が複数種類存在する場合、端末が端末暗号文に所望の秘密情報の種類を指定し、かつ同一ラウンドにおいては常に同じ端末乱数を端末暗号文に使用し、センタは、同一ラウンドにおいて同一の端末乱数が使用された端末暗号文に対して指定された種類の秘密情報を端末乱数より生成した共通鍵により暗号化して配送する構成とした。このような構成にしたことにより、秘密情報が複数種類存在しても複製端末を発見することができる。

【0023】また、端末がセンタからの通信を受信できない場合、センタに対して現在のラウンド番号を問い合わせる問い合わせ手段を端末に備え、問い合わせた結果、端末とセンタのラウンド番号が異なる場合に、端末

がセンタに再送を要求する再送要求手段とを備えた構成とした。このような構成にしたことにより、端末がセンタからの情報を受信できない場合にも、複製端末の発見および秘密情報の配布を再開できる。

【0024】また、通信システムを、同報通信システムとした。このような構成にしたことにより、センタ乱数を同報通信して通信量を削減でき、グループ鍵を用いた暗号化同報通信も実現できる。

【0025】また、端末乱数生成手段を、同じ乱数を出力する乱数生成器を他に作成できず、かつ偶然他の乱数生成器の出力と同じ出力となる確率が無視できる出力長を持つという条件を満たすものとした。このような構成にしたことにより、一定の攻撃に対して充分安全を確保できる。

【0026】また、グループ鍵の配布の途中において、複製端末が発見された場合、グループ鍵を未配布の端末の端末公開鍵（センタが端末秘密鍵を管理している場合は端末秘密鍵）によりグループ鍵を暗号化して未配布の端末に配布する手段を備えた。このような構成にしたことにより、早期にグループ通信を再開することができる。ただし、端末数に依存した通信量が必要となるので、端末数が小さい場合にのみ有効である。

【0027】

【発明の実施の形態】以下、本発明の実施の形態について、図1～図8を参照しながら詳細に説明する。

【0028】（第1の実施の形態）本発明の第1の実施の形態は、センタと複数台の端末が、個々のセッション鍵で暗号通信する通信網により接続された通信システムにおいて、センタが各端末に新規セッション鍵を配布する際に、端末で発生した乱数が複製困難なことを利用して端末IDの重複を検査することで複製端末を発見する方法である。

【0029】図1は、本発明の第1の実施の形態における複製端末発見方法の流れ図である。図1において、センタCは、各端末にセッション鍵を配布する機関である。通信路Nは、暗号通信可能な無線または有線の通信媒体である。端末Tiは、センタCとセッション鍵で暗号通信を行なう通信装置である。端末は複数台あり、iは各端末にユニークな端末IDである。端末は1台でもよい。フェーズ#1は、複製端末を発見するための手続きを行なう段階である。フェーズ#2は、センタCから端末Tiにセッション鍵を配送するための手続きを行なう段階である。

【0030】図2は、本発明の第1の実施の形態における複製端末発見方法に用いるセンタの構成図である。図2において、乱数生成手段1は、擬似乱数を生成する手段である。送信手段2は、有線または無線でデータを端末に送信する手段である。公開鍵暗号復号手段3は、センタCの公開鍵で暗号化された暗号文を復号する手段である。認証文検証手段4は、端末秘密鍵で暗号化された

認証文を端末公開鍵で復号して検証する手段である。データベース手段5は、端末との交信記録をまとめたデータベースである。検出手段6は、データベースを検索して端末の重複を検出する手段である。共通鍵生成手段7は、端末との共通鍵を端末乱数から生成する手段である。共通鍵暗号化手段8は、端末との共通鍵でセッション鍵を暗号化する手段である。

【0031】図3は、本発明の第1の実施の形態における複製端末発見方法に用いる端末の構成図である。図3において、乱数生成手段1は、複製困難な擬似乱数を生成する手段である。送信手段2は、有線または無線でデータをセンタに送信する手段である。共通鍵生成手段7は、センタとの共通鍵を端末乱数から生成する手段である。共通鍵暗号復号手段9は、共通鍵で暗号化されたセッション鍵を復号する手段である。認証文生成手段10は、端末乱数とセンタ乱数を端末秘密鍵で暗号化して認証文を生成する手段である。公開鍵暗号化手段11は、認証文と端末乱数をセンタ公開鍵で暗号化する手段である。

【0032】図4は、本発明の第1の実施の形態における複製端末発見方法の複製端末発見フェーズ（フェーズ#1）の流れ図である。図5は、本発明の第1の実施の形態における複製端末発見方法のセッション鍵配送フェーズ（フェーズ#2）の流れ図である。

【0033】上記のように構成された本発明の第1の実施の形態における複製端末発見方法の動作を説明する。最初に、図1を参照して、複製端末発見方法の原理を説明する。複製端末発見方法は、センタCにしか解読できないように暗号化されて端末Tiから送信された端末乱数R_iと端末認証文を、センタCで検証し、端末認証文が正しく、かつ現時点において同じ端末IDを持つ端末から異なる端末乱数R_iが送信されていない場合にのみ、この端末乱数R_iに依存して端末Tiにセッション鍵SK_iを与えるプロトコルである。ただし、上付きのbはラウンド番号であり、ベキ乗の意味ではない。ラウンドは、セッション鍵の有効期間である。ラウンド番号は、端末ごとに独立であるので、厳密には端末IDで識別できるようにすべきであるが、記載が煩雑になり、紛れることもないので、単にbと書く。端末IDのiやラウンド番号bを省略することもある。

【0034】複製端末発見方法は、複製端末発見フェーズとセッション鍵配送フェーズの2つのフェーズからなる。複製端末発見フェーズ（フェーズ#1）では、センタCは、チャレンジレスポンス認証により、端末Tiと、その端末TiがセンタCの公開鍵により暗号化して配信した端末乱数R_iを認証する。この端末乱数R_iを用いて、端末Tiと共通鍵を共有する。センタCは、データベースを検索して、端末識別符号の重複を検査する。同一端末IDを持ち、異なる端末乱数を送信した端末Ti'を検出すると、この端末IDを持つオリジナル端末T

iの複製端末が存在すると判定できる。セッション鍵配送フェーズ（フェーズ#2）では、センタCは、複製端末のない端末Tiに対して、セッション鍵SK_iを共通鍵CK_iにより暗号化して配送する。

【0035】チャレンジ-レスポンス認証を説明する。センタCは、センタ乱数Z_iを生成して、チャレンジCH_Aとして端末Tiに送信する。端末Tiは、センタCから受信したセンタ乱数Z_iと、自身が生成した端末乱数R_iに対して、自身の秘密鍵により生成した認証文を、レスポンスRESとしてセンタCに送信する。これをセンタCが検証することにより、端末Tiとその端末乱数R_iを認証する。ここで、センタCは、端末Tiとその端末乱数R_iとの対応を確認する。デジタル署名を用いる場合は、センタCに各端末の秘密鍵を保管する必要がなく、鍵管理が容易となる。

【0036】端末乱数R_iの暗号化を説明する。同じ端末秘密鍵を保持する複製端末に対して端末乱数R_iを秘密にするために、センタ公開鍵により端末乱数R_iを暗号化する。または、Diffie-Hellman鍵共有法のような乱数を用いた方法により共有した鍵を、端末乱数の代わり利用する。

【0037】データベースの検索を説明する。センタCは、データベースを検索して、端末Tiに既にセッション鍵SK_iを配送済みか確認する。配送済みならば、配送に使用した端末乱数R_iと、送信されてきた端末乱数R_iとを比較して、不一致ならば、端末Tiの複製端末が存在すると判断する。端末Tiは、同一ラウンドでは同じ乱数を用いるので、複製端末が存在しない限り、異なる端末乱数R_iを用いたレスポンスRESは来ない。ただし、端末乱数R_iと端末乱数R_iのどちらが複製端末の乱数であるかは区別できない。また、複製端末が複数ならば、端末乱数R_iと端末乱数R_iが共に複製端末の乱数である可能性があるが、複製端末が単数複数いずれの場合でも、複製端末発見方法により複製端末の存在を検出できる。

【0038】共通鍵CK_iの生成を説明する。正しく認証され、かつ複製端末が発見されない端末Tiと、センタCは、その端末Tiの端末乱数を使って共通鍵を共有する。ここで、共通鍵の生成には、センタCと端末乱数の保持者のみが生成できる方法を使う必要がある。最も単純な方法は、端末乱数をそのまま共通鍵として用いる方法である。

【0039】セッション鍵SK_iの暗号化を説明する。センタCは、共通鍵CK_iを用いて、セッション鍵SK_iを暗号化する。端末Tiは、センタCと同様に、端末乱数R_iより共通鍵CK_iを生成する。共通鍵CK_iを使ってセッション鍵SK_iを復号する。端末秘密鍵Siが漏洩しても、端末乱数R_iがなければ、共通鍵CK_iは生成できないため、オリジナル端末と複製端末の集合の中で、セッション鍵SK_iを得ることができるのは、1台のみとな

る。また、ここで使う暗号は、レスポンスRES_iの場合と異なり、共通鍵暗号でよい。また、必要であればMAC（Message Authentication Code：メッセージ認証符号）を併用して、改ざんや成りすましを検出する機能を追加できる。

【0040】セッション鍵SK_iの更新を説明する。センタCは、一時横流しによるセッション鍵の漏洩に対処するために、定期的にセッション鍵を更新して、複製端末発見方法を実行する必要がある。この期間が短いほど、早く複製端末を発見・無効化できる。

【0041】セッション鍵SK_iが複数の場合を説明する。セッション鍵の種類が複数の場合は、各端末Tiは、同一ラウンドであれば同じ端末乱数を用いて、セッション鍵の種類を指定したレスポンスRES_iを送信する。センタCは、データベースより乱数が同じことを確認して、端末Tiが指定したセッション鍵を、同じ乱数による鍵で暗号化して配送する。

【0042】未受信対策を説明する。端末Tiが電源オフや、通信できない地域へ移動したことなどにより、チャレンジCH_Aやセッション鍵を受信できない場合のために、現在のラウンド番号をセンタに問い合わせる機能を、端末Tiに付加する。ラウンドが進んでいる場合に、端末Tiはセンタに再送を要求する。

【0043】以上のようにすることにより、複製端末を発見できる。正規の端末Tiが先にレスポンスRES_iを送信し、複製端末がレスポンスRES_iを送信しない場合には、複製端末は発見できないが、複製端末はセッション鍵を得ることができないので、実質的に無効化することができる。

【0044】第2に、図2、図3、図4を参照しながら、複製端末発見の手順（フェーズ#1）の各ステップについて説明する。準備段階において、図示していない信頼できるシステム管理者は、センタ秘密鍵Scと、センタ公開鍵Ycと、各端末Tiの端末秘密鍵Siと、端末公開鍵Yiを生成する。センタCに、センタ秘密鍵Scと端末公開鍵Yiを秘密に配布する。各端末Tiに、対応する端末秘密鍵Siとセンタ公開鍵Ycを秘密に配布する。

【0045】図4に示すフェーズ#1-1で、図1に示すセンタCは、図2の乱数生成手段1でセンタ乱数Z_iを生成する。端末Tiに、セッション鍵の更新通知を兼ねるチャレンジCH_A=Z_i

を送信手段2により送信する。

【0046】フェーズ#1-2で、図3に示す端末Tiは、図3の乱数生成手段1により、端末乱数R_iを生成する。自身の端末秘密鍵Siを用いて、端末IDのiと、センタCからチャレンジCH_Aとして送られたセンタ乱数Z_iと、端末乱数R_iとに対するデジタル署名Sig(Si, (i || Z_i || R_i))を、認証文生成手段10で生成する。ただし、(x || y)は、xを上位桁とし、yを下位桁

とする。符号の連接を示す。SIG(x, y)は、鍵xを使ってyのデジタル署名を計算することを示す。このデジタル署名を、端末認証文D_iとする。

【0047】センタ公開鍵Y_cを用いて、端末IDのiと、端末乱数R_iと、端末認証文D_iとに対する端末暗号文

$$E_i = Y_c[i \parallel R_i \parallel D_i]$$

$$= Y_c[i \parallel R_i \parallel \text{SIG}(S_i, (i \parallel Z_i \parallel R_i))]$$

を、公開鍵暗号化手段11で生成する。ただし、x[y]は、yを鍵xで暗号化することを示す。これを、センタCに、セッション鍵要求通知を兼ねるレスポンス

$$\text{RES}_i = E_i = Y_c[i \parallel R_i \parallel D_i]$$

$$= Y_c[i \parallel R_i \parallel \text{SIG}(S_i, (i \parallel Z_i \parallel R_i))]$$

として、送信手段2で送信する。

【0048】フェーズ#1-3で、図2のセンタCは、図示しない受信手段で、端末T_iからのレスポンスRES_iを受信し、公開鍵暗号復号手段3で、センタ秘密鍵S_cを使ってレスポンスRES_iを復号して、端末乱数R_iを得る。認証文検証手段4で、端末T_iの端末公開鍵Y_iを用いて、SIG(S_i, (i \parallel Z_i \parallel R_i))を検証する。検証結果が正しい場合は、端末T_iと端末乱数R_iを認証したとして受付けて、フェーズ#1-4へ進む。検証結果が不正の場合は、プロトコルを終了する。

【0049】フェーズ#1-4で、センタCは、検出手段6により、端末IDをキーとして、端末IDと配送に用いた乱数を関連付けて登録したデータベースが格納されたデータベース手段5を参照する。配送に用いた乱数が登録されていない、つまりセッション鍵SK_iが未配送の場合は、データベースに端末乱数R_iを記録して、フェーズ#1-5へ進む。配送に用いた乱数が登録されている、つまりセッション鍵SK_iが配送済みの場合は、データベースに記録された端末乱数R_i'と受信した端末乱数R_iが等しいならフェーズ#1-5へ進む。異なるなら、複製端末を発見したと判断して、プロトコルを終了する。

【0050】フェーズ#1-5で、センタCは、図2の共通鍵生成手段7により、端末乱数R_iを共通鍵CK_iとする。

【0051】第3に、図2、図3、図5を参照しながら、セッション鍵配送の手順（フェーズ#2）の各ステップを説明する。重複が検出されなかった端末に対してのみ、センタCはセッション鍵を配送する。

【0052】図5に示すフェーズ#2-1で、センタCは、共通鍵暗号化手段8により、セッション鍵SK_iを共通鍵CK_iで暗号化したセンタ暗号文

$$EC_i = CK_i[SK_i]$$

を生成して、送信手段2により端末T_iに送信する。

【0053】フェーズ#2-2で、端末T_iは、図示しない受信手段により、センタ暗号文EC_i (=CK_i[SK_i])を受信する。端末乱数R_iを共通鍵CK_iとして、図

3の共通暗号復号手段9により、センタ暗号文EC_i (=CK_i[SK_i])を復号し、セッション鍵SK_iを得る。端末T_iが、センタ暗号文EC_i (=CK_i[SK_i])を受信できなかった場合は、フェーズ#1-2において生成したレスポンスRES_iを、センタCに再送する。

【0054】第4に、乱数生成器の条件を説明する。端末に組込まれる乱数生成手段が満たすべき条件は、「同じ乱数を出力する乱数生成器を他に作成できないこと、かつ偶然他の乱数生成器の出力と同じ出力となる確率が無視できる出力長を持つこと」である。これは、乱数生成器の構造は複製できても、乱数またはシードの元となる状態が複製できないものであって、かつ出力が128bit程度あるものであれば満たされる。したがって、次の128bit乱数生成器は条件を満たす。

- ・ホワイトノイズなどを利用した真性乱数生成器
- ・予測困難な常に変化する各端末固有の状態により更新されるシードを入力とする擬似乱数生成器または擬似乱数生成ソフトウェア

【0055】このようなシードとして、以下のものやその組合せがある。

- ・端末のメモリの状態やシステムクロックの値
- ・端末の動作に関する時間、時刻、回数

【0056】第5に、安全性について説明する。複製端末発見方法は、複製端末の発見を目的とする。攻撃者は複製端末を偽造して暗号通信を解読することを目的とする。まず、複製端末発見方法において想定される攻撃について説明する。複製端末発見方法では、既に攻撃者が複製対象となるオリジナル端末の秘密鍵を保持していることを前提とした攻撃を想定する。端末秘密鍵を不正に取得できる機会には、メンバが自身の端末を解析する場合と、メンバが自身の端末から目を離している間（紛失・充電時など）に攻撃者が端末を解析する場合と、複数のメンバの結託により他のメンバの秘密鍵を作成する場合などがある。この前提において、攻撃者は、複製端末を偽造して暗号通信の解読を試みる。

【0057】攻撃は、オリジナル端末はそのままに、攻撃者が残りの秘密情報（セッション鍵、乱数）を入手できる横流し攻撃と、オリジナル端末を改変するか、別の端末（複製端末）に入れ替えてしまうことにより、オリジナル端末を無効化する改変攻撃に分けられる。

【0058】横流し攻撃のうち、一時横流し攻撃では、ある時点において、オリジナル端末のセッション鍵か、このセッション鍵を得るための乱数が漏洩し、攻撃者が複製端末を偽造する。常時横流し攻撃では、定期的に、オリジナル端末のセッション鍵か、このセッション鍵を得るための乱数を、不正なメンバが横流しして、攻撃者が複製端末を偽造する。改変攻撃は、オリジナル端末を改変するか、複製端末に入れ替えることにより、オリジナル端末を無効化し、複製端末を使用しても発見させない攻撃である。

【0059】本実施の形態における複製端末発見方法は、一時横流し攻撃に対して複製端末を発見することを目的とする。常時横流し攻撃および改変攻撃は、以下の理由により考慮する必要がないと考える。

【0060】常時横流し攻撃は、横流しの頻度に依存して不正なメンバの通信コストや不正発覚の可能性が増加するため、不正なメンバは容易に実行できないと考えられる。

【0061】改変として、具体的に以下の2つの場合が考えられる。1つ目は、オリジナル端末の使用者が目を離れた隙などに、攻撃者がオリジナル端末を複製端末と入れ替える場合である。この複製端末は、他の複製端末と乱数が同期しているとすれば、改変されたオリジナル端末を使用し続ける限り、乱数による複製端末の発見はできない。しかし、常時端末を使用しているオリジナル端末の使用者に気付かれない複製端末を偽造することは、時間やコストの面から難しいと考える。また、物理的な改変を検出することは、情報の複製を検知することに比べ、一般に容易かつ低コストであるので、これを併用して対処できる。

【0062】2つ目は、オリジナル端末の使用者が、攻撃者または攻撃者に協力する不正なメンバの場合である。オリジナル端末の乱数生成器を複製端末と同期するように改変するか、同期する複製端末に入れ替えることにより、オリジナル端末を無効化する。1つ目より、不正なメンバの協力により成功する可能性が高い。しかし、不正発覚時に所有する改変した端末または複製端末により、不正なメンバであることを特定されてしまうため、容易に実行できない。また、端末を故障させて常に同じ乱数を出力させることにより、複製端末と乱数生成器を同期させる攻撃は、一定期間ログを保存・解析することにより検出できる。

【0063】以上の検討より、複製端末発見方法では、以下の仮定が満たされるとする。このとき、複製端末発見方法は安全である。

1. 攻撃者は複製対象となる端末の秘密鍵を保持する。
2. 一時横流し攻撃が可能である。
3. 常時横流し攻撃および改変攻撃は困難である。
4. 端末に上に定義した乱数生成器が組込まれる。
5. オリジナル端末はメンバにより使用される。
6. 共通鍵暗号方式、公開鍵暗号方式、MACおよびデジタル署名方式は安全である。

【0064】仮定1と2は現実的に起こりうる。一方、仮定3の攻撃は理論的には可能だが、攻撃者の負担が大きく、現実的にはあまり起こりえないと予測されるため考慮しない。仮定3～5により、オリジナル端末に対する入替えや改変は行われず、かつ前述の乱数生成器をメンバが必ず使用すると仮定できる。仮定6については、共通鍵暗号方式として鍵長128bit程度の共通鍵暗号を利用し、公開鍵暗号方式として鍵長1024bit程度のRSA暗号

やElGamal暗号や、鍵長160bit程度の楕円ElGamal暗号を利用し、MACとして鍵長128bit程度の共通鍵暗号や、出力128bit程度の鍵付きハッシュ関数を利用し、デジタル署名として鍵長1024bit程度のDSA署名やRSA署名や、鍵長160bit程度の楕円DSA署名を利用することにより満たされる。

【0065】一時横流し攻撃に対する安全性について説明する。攻撃者が入手可能な情報は、オリジナル端末の秘密鍵と、攻撃に成功した時点のラウンドのセッション鍵と、対応する乱数である。以上により偽造された単数または複数の複製端末と、オリジナル端末が存在すると考える。

【0066】攻撃時点のラウンドのセッション鍵が更新されたとき、オリジナル端末が先にレスポンスRESを送信し、後から複製端末がレスポンスRESを送信した場合は、乱数の違いから複製端末を発見できる。レスポンスRESを送信しなければ、複製端末はセッション鍵を得られないため、実質的に無効化される。一方、複製端末が先にレスポンスRESを送信し、後からオリジナル端末がレスポンスRESを送信した場合は、乱数の違いから複製端末を発見できる。

【0067】つまり、オリジナル端末と複製端末の集合の内、セッション鍵を得られるのは常に1台であり、この内1台でもレスポンスRESを送信すれば、複製端末を発見または無効化できる。ここで、前述の仮定により、集合の内最低1台はレスポンスRESを送信するので、この攻撃に対して複製端末発見方法は安全である。

【0068】他の攻撃に対する安全性について説明する。偽造以外には、レスポンスRESを再送するReplay Attackがある。レスポンスRESに対して、センタは、共通鍵により暗号化したセッション鍵を配送するので、通信量は増加するが、乱数が無ければ復号はできないので問題ない。また、仮定により、暗号化関数と認証文生成関数が安全なので、暗号文の解読・レスポンスRESに対する成りすまし・改ざんは困難である。改変攻撃で述べたような端末を故障させる攻撃に対しては、センタが過去のデータベースを記録・検査すれば対処できる。したがって、過去の全てのラウンドのデータベースを保持・検査することが最も安全であるが、実際にはコストと安全性のトレードオフで、一定期間のデータベースのみを保持することになる。センタによる端末の陥れに関しては、センタが端末の秘密鍵を保持していないために困難である。

【0069】第6に、従来技術と比較して違いを説明する。本方法は、公開鍵 e 33bit、法 n ・秘密鍵1024bitのRSAとし、従来法は、 p を1024bit、 q を160bit、ハッシュ関数の出力を128bitとして比較する。ただし、RSAは一般に良く用いられる中国人剰余定理により秘密鍵の演算を高速化する方法の利用を考慮する。演算量は、全パラメータ1024bitのベキ乗剰余1回を1として換算する。ま

た、 n は端末総数、 k は結託しきい値である。共通鍵暗号・MACの演算量とIDのサイズは無視する。このとき、本方法はレスポンス検証の演算量以外は従来法より効率

的である。

【0070】

	従来方法	本方法
チャレンジ通信量	$(1024\text{bit} \times (k+2)) \times n$	$128\text{bit} \times n$
チャレンジ演算量	$0.16 \times (2k+1)$	なし
レスポンス通信量	2176bit	1024bit
レスポンス生成演算量	0.48	0.28
レスポンス検証演算量	0.16	0.28
データベースサイズ	$2176\text{bit} \times n$	$128\text{bit} \times n$

【0071】上記のように、本発明の第1の実施の形態では、複製端末発見方法を、センタと複数台の端末が、個々のセッション鍵で暗号通信する通信網により接続された通信システムにおいて、センタが各端末に新規セッション鍵を配布する際に、端末で発生した乱数が複製困難なことを利用して端末IDの重複を検査することで複製端末を発見する構成としたので、複製端末の存在を自動的に検出して排除できる。

【0072】（第2の実施の形態）本発明の第2の実施の形態は、センタと複数台の端末が、共通のグループ鍵により暗号通信する同報通信網により接続された通信システムにおいて、センタが各端末に新規グループ鍵を配布する際に、端末で発生した乱数が複製困難なことを利用して端末IDの重複を検査することで複製端末を発見する方法である。

【0073】図6は、本発明の第2の実施の形態における複製端末発見方法の流れ図である。図6において、センタCは、各端末にグループ鍵を配布する局である。通信路Nは、同報暗号通信可能な無線または有線の通信媒体である。端末T_iは、センタCとグループ鍵で暗号通信を行なう通信装置である。端末は複数台あり、 i は各端末にユニークな端末IDである。端末は1台でもよい。フェーズ#1は、複製端末を発見するための手続きを行なう段階である。フェーズ#2は、センタCから端末T_iにグループ鍵を配送するための手続きを行なう段階である。本発明の第2の実施の形態における複製端末発見方法のシステム構成は、基本的に第1の実施の形態と同じである。

【0074】図7は、本発明の第2の実施の形態における複製端末発見方法の複製端末発見フェーズ（フェーズ#1）の流れ図である。図8は、本発明の第2の実施の形態における複製端末発見方法のグループ鍵配送フェーズ（フェーズ#2）の流れ図である。

【0075】上記のように構成された本発明の第2の実施の形態における複製端末発見方法の動作を説明する。最初に、図6を参照して、複製端末発見方法の全体の動作を説明する。準備段階において、信頼できるセンタCは、自身のセンタ秘密鍵S_cとセンタ公開鍵Y_cと、各端末の端末秘密鍵S_iを生成して、各端末に、対応する端末秘密鍵S_iとセンタ公開鍵Y_cを秘密に配布する。

【0076】複製端末発見方法は、複製端末発見フェーズとグループ鍵配送フェーズの2つのフェーズからなる。複製端末発見フェーズ（フェーズ#1）では、センタCは、チャレンジ-レスポンス認証により、端末T_iと、その端末T_iがセンタCの公開鍵により暗号化して送信した端末乱数R_iを認証する。この端末乱数R_iを用いて、端末T_iと共通鍵を共有する。センタCは、データベースを検索して、端末IDの重複を検査する。同一端末IDを持ち、異なる端末乱数を送信した端末T_i'を検出すると、この端末IDを持つオリジナル端末T_iの複製端末が存在すると判定できる。グループ鍵配送フェーズ（フェーズ#2）では、センタCは、複製端末のない端末T_iに対して、グループ鍵GK_iを共通鍵CK_iにより暗号化して配送する。第1の実施の形態と表現を合わせるために、チャレンジ-レスポンス認証による形態を示したが、本発明においては、センタによるチャレンジは必須でないため、実装するシステムにおける制限や安全性より効率を重視する場合は、センタはチャレンジを送信しなくても構わない。

【0077】複製端末発見フェーズ（フェーズ#1）において、センタCは、全端末に、同報通信網Nを用いて、共通のチャレンジCHAを同報する。各端末が、共通のチャレンジCHAに対して、個別のレスポンスRESを返す。

【0078】チャレンジ-レスポンス認証を説明する。端末は、センタからの全端末共通のセンタ乱数Z^bと、自身が生成した端末乱数R_iに対して、自身の端末秘密鍵により生成したMACをレスポンスRESとして、センタに送信する。これをセンタが検証することにより、端末とその端末乱数R_iを認証する。ここで、センタは、端末とその端末乱数との対応を確認する。MACでは、センタが全端末の端末秘密鍵を保管する必要があるが、処理が軽い。同報通信網を利用したことにより、チャレンジCHAを、各端末で共通化できる。

【0079】端末乱数R_iの暗号化を説明する。同じ端末秘密鍵を保持する複製端末に対して、端末乱数を秘密にするため、センタ公開鍵により端末乱数を暗号化する。または、Diffie-Hellman鍵共有法のような乱数を用いた方法により共有した鍵を、端末乱数の代わりに利用する。

【0080】データベースの検索を説明する。センタは、データベースを検索して、端末T_iに、既にグループ鍵G_K^bを配送済み（端末乱数R_i^bが登録されている）か確認する。配送済みならば、配送に使用した端末乱数R_i^bと、送信されてきた端末乱数R_i^bを比較して、不一致ならば、端末T_iの複製端末が存在すると判断する。端末T_iは、同一ラウンドでは同じ乱数を用いるので、複製端末が存在しない限り、異なる端末乱数R_i^bを用いたレスポンスRESは来ない。ただし、端末乱数R_i^bと端末乱数R_i^bのどちらが複製端末の乱数であるかは区別できない。また、複製端末が複数ならば、端末乱数R_i^bと端末乱数R_i^bが共に複製端末の端末乱数である可能性があるが、いずれの場合でも、複製端末発見方法により複製端末を発見できる。

【0081】共通鍵CK_i^bの生成を説明する。センタは、正しく認証され、かつ複製端末が発見されない端末と、その乱数により共通鍵を共有する。ここで、共通鍵の生成には、センタと端末乱数の保持者のみが生成できる方法を使用する必要がある。最も単純な方法は、端末乱数をそのまま共通鍵として用いる方法である。

【0082】グループ鍵配送フェーズ（フェーズ#2）において、センタCは、複製端末のない端末T_iに対して、グループ鍵G_K^bを共通鍵CK_i^bにより暗号化して配送する。グループ鍵G_K^bの暗号化を説明する。センタは、共通鍵CK_i^bを用いて、グループ鍵G_K^bを暗号化する。端末T_iは、センタと同様に、端末乱数R_i^bより共通鍵CK_i^bを生成する。共通鍵CK_i^bで、グループ鍵G_K^bを復号する。端末秘密鍵S_iが漏洩しても、端末乱数R_i^bがなければ、共通鍵CK_i^bを生成できないため、オリジナル端末と複製端末の集合の中で、グループ鍵G_K^bを得ることができるのは1台のみとなる。また、必要であればMACを併用して、改ざんや成りすましを検出する機能を追加できる。

【0083】グループ鍵G_K^bの更新を説明する。センタは、一時横流しによるグループ鍵の漏洩に対処するために、定期的にグループ鍵を更新して複製端末発見方法を実行する必要がある。この期間が短いほど、早く複製端末を発見・無効化できる。

【0084】グループ鍵G_K^bが複数の場合を説明する。グループ鍵の種類が複数の場合は、各端末は、同一ラウンドであれば同じ乱数を用いて、グループ鍵の種類を指定したレスポンスRESを送信する。センタは、データベースより、端末乱数が同じことを確認して、端末が指定したグループ鍵を、同じ乱数により暗号化して配送する。

【0085】未受信対策を説明する。端末が電源オフや通信できない地域へ移動したことなどにより、チャレンジCHAやグループ鍵を受信できない場合のために、現在のラウンド番号をセンタに問い合わせる機能を端末に付加し、ラウンドが進んでいる場合に、端末はセンタに再

送を要求する。

【0086】以上のようにすることにより、複製端末を発見できる。正規の端末が先にレスポンスRESを送信し、複製端末がレスポンスRESを送信しない場合には、複製端末は発見できないが、複製端末はグループ鍵を得ることができないので、実質的に無効化することができる。第1の実施の形態との違いは、デジタル署名の代わりにMACを使用しているため、処理が高速であること、同報通信網の利用により、チャレンジCHAを各端末で共通化できるので、通信量が少ないこと、セッション鍵の代わりにグループ鍵を配送していることである。安全性の違いは、センタは各端末の端末秘密鍵を保管するため、信頼できる機関であることが必要である点である。

【0087】第2に、図2、図3、図7を参照しながら、複製端末発見（フェーズ#1）の各手順を説明する。図7のフェーズ#1-1で、センタCは、図2の乱数生成手段1によりセンタ乱数Z^bを生成し、全端末に、グループ鍵の更新通知を兼ねるチャレンジCHA^b=Z^b

を送信手段2により送信する。ただし、上付きのbはラウンド番号であり、ベキ乗の意味ではない。ラウンドは、グループ鍵の有効期間である。

【0088】フェーズ#1-2で、各端末T_iは、図3の乱数生成手段1により、端末乱数R_i^bを生成する。認証文生成手段10により、自身の端末秘密鍵S_iを用いて、端末IDであるiと、センタCからのチャレンジCHA^bであるセンタ乱数Z^bと、端末乱数R_i^bに対するMAC（Message Authentication Code：メッセージ認証符号）を生成して、端末認証文D_i^bとする。すなわち、 $D_i^b = \text{MAC}(S_i, (i \parallel Z^b \parallel R_i^b))$

を生成する。ただし、MAC(x, y)は、鍵xを使って、yのメッセージ認証符号を計算することを示す。公開鍵暗号化手段11により、センタCのセンタ公開鍵Y_cを用いて、端末IDと、端末乱数R_i^bと、端末認証文D_i^bに対する端末暗号文

$$E_i^b = Y_c[i \parallel R_i^b \parallel D_i^b] \\ = Y_c[i \parallel R_i^b \parallel \text{MAC}(S_i, (i \parallel Z^b \parallel R_i^b))]$$

を生成する。これを、センタCに、セッション鍵要求通知を兼ねるレスポンス

$$\text{RES}_i^b = E_i^b = Y_c[i \parallel R_i^b \parallel D_i^b] \\ = Y_c[i \parallel R_i^b \parallel \text{MAC}(S_i, (i \parallel Z^b \parallel R_i^b))]$$

として、送信手段2により送信する。

【0089】フェーズ#1-3で、図2のセンタCは、図示しない受信手段により、端末T_iからのレスポンスRES_i^bを受信する。公開鍵暗号復号手段3により、自身のセンタ秘密鍵S_cを使って、レスポンスRES_i^bを復号して、端末乱数R_i^bを得る。認証文検証手段4により、端末T_iの端末秘密鍵S_iを用いて、端末認証文D_i^bを検証する。検証結果が正しい場合は、端末T_iと端末乱数R_i^b

b を認証したとして受付けて、フェーズ#1-4へ進む。検証結果が不正の場合は、プロトコルを終了する。

【0090】フェーズ#1-4で、センタCは、端末IDと、グループ鍵の配送に用いた乱数とを関連付けて登録したデータベースが格納されているデータベース手段5を、検出手段6により、端末IDをキーとして参照する。グループ鍵 GK^b が未配送（端末乱数が登録されていない）の場合は、データベースに、端末乱数 R^b を記録して、フェーズ#1-5へ進む。グループ鍵 GK^b が配送済み（端末乱数が登録されている）の場合は、データベースに記録された端末乱数 R^b と、受信した端末乱数 R^b が等しいなら、フェーズ#1-5へ進む。異なるなら、複製端末を発見したと判断して、プロトコルを終了する。

【0091】フェーズ#1-5で、センタCは、共通鍵生成手段7により、端末乱数 R^b を共通鍵 CK^b とする。

	従来方法	本方法	条件
チャレンジ通信量	1024bit×(k+2)	128bit	
チャレンジ演算量	0.16×(2k+1)	なし	
レスポンス通信量	2176bit	1024bit	
レスポンス生成演算量	0.48	0.03	
レスポンス検証演算量	0.16	0.25	本方法の検証はMAC
データベースサイズ	2176bit×n	128bit×n	

【0095】本方法では、レスポンス検証の演算量以外は従来法より効率的である。特に、センタが信頼でき、かつ全体の通信量と端末の演算量が少ないという条件は移動体通信に適している。RSAの代わりに楕円ElGamal暗号を用いることにより通信量をさらに削減することができるが、端末の演算量はRSAの場合より増加する。従来法では、PKIにおける端末の公開鍵の証明書を検証する必要がある点が利点としてあるが、センタは予め検証した公開鍵を保管しておくことが可能なので、証明書の検証の演算量は無視できる。

【0096】グループに属する端末数が多いグループ通信システムにおいて、グループ鍵 GK^b を配布中に複製端末を発見した場合、現在のグループ鍵 GK^b を用いた暗号通信を中止し、早期に GK^b を用いた暗号通信を再開する必要がある。しかしながら、グループ鍵 GK^b の配布に、端末ごとに双方向通信を必要とし、全端末にグループ鍵 GK^b を配布完了するまでに時間がかかる場合がある。そこで、残りの端末の複製端末の検査は後回しとして、未検査の端末T_iに対して、端末秘密鍵S_iまたは端末公開鍵Y_iによりグループ鍵 GK^b を暗号化して配布することにより、高速に配布することが可能となる。

【0097】上記のように、本発明の第2の実施の形態では、複製端末発見方法を、センタと複数台の端末が、共通のグループ鍵により暗号通信する同報通信網により接続された通信システムにおいて、センタが各端末に新規グループ鍵を配布する際に、端末で発生した乱数が複製困難なことを利用して端末IDの重複を検査することで

【0092】第3に、図2、図3、図8を参照しながら、グループ鍵配送（フェーズ#2）の各手順を説明する。図8に示すフェーズ#2-1で、センタCは、共通鍵暗号化手段8により、共通鍵 CK^b を用いて、グループ鍵 GK^b を暗号化したセンタ暗号文 $EC^b = CK^b[GK^b]$

を生成して、送信手段2により、端末T_iに送信する。

【0093】フェーズ#2-2で、図3の端末T_iは、図示していない受信手段により、センタ暗号文 $EC^b (= CK^b[GK^b])$ を受信する。共通鍵暗号復号手段9により、端末乱数 R^b を共通鍵 CK^b とし、センタ暗号文 $EC^b (= CK^b[GK^b])$ を復号して、グループ鍵 GK^b を得る。端末T_iが、センタ暗号文 $EC^b (= CK^b[GK^b])$ を受信できなかった場合は、フェーズ#1-2において生成したレスポンスRESを、センタCに再送する。

【0094】従来技術と比較して違いを説明する。

複製端末を発見する構成としたので、複製端末の存在を自動的に検出して排除して、グループ鍵を配布できる。

【0098】

【発明の効果】以上の説明から明らかなように、本発明では、センタと複数台の端末を含む通信システムの複製端末発見方法を、センタで、ラウンドごとにセンタ乱数を生成し、前回ラウンドにおける秘密情報の更新通知とセンタ乱数をチャレンジとして端末に送信し、端末で、チャレンジを受信し、ラウンドごとの端末乱数を生成し、センタ乱数と端末乱数に対する端末認証文を端末秘密鍵により生成し、端末認証文と端末乱数とをセンタ公開鍵で暗号化して端末暗号文としてセンタに送信し、センタCで、センタ秘密鍵で端末暗号文を復号して端末認証文と端末乱数とを得て、端末公開鍵で端末認証文を検証し、秘密情報の配送に使用した端末乱数と、端末IDとを、対応させて登録したデータベースを検索して、同一端末IDでかつ異なる端末乱数が登録されている重複登録の有無を検査し、端末認証文の検証結果が正しく、かつ重複登録が無い端末の端末乱数をデータベースに登録し、この端末乱数を用いて、共通鍵を生成し、共通鍵により秘密情報を暗号化してセンタ暗号文として端末に送信し、端末で、センタ暗号文を受信し、端末乱数から共通鍵を生成し、センタ暗号文を共通鍵により復号して秘密情報を得る構成としたので、センタは自動的に複製端末の存在を検知でき、発見を恐れて複製端末が乱数を送らない場合には、複製端末は秘密情報を入手できないので無効化することができるという効果が得られる。

【図面の簡単な説明】

【図 1】 本発明の第 1 の実施の形態における複製端末発見方法の流れ図、

【図 2】 本発明の第 1 の実施の形態における複製端末発見方法で使用するセンタの構成図、

【図 3】 本発明の第 1 の実施の形態における複製端末発見方法で使用する端末の構成図、

【図 4】 本発明の第 1 の実施の形態における複製端末発見方法の複製端末発見フェーズ（フェーズ # 1）の流れ図、

【図 5】 本発明の第 1 の実施の形態における複製端末発見方法のセッション鍵配送フェーズ（フェーズ # 2）の流れ図、

【図 6】 本発明の第 2 の実施の形態における複製端末発見方法の流れ図、

【図 7】 本発明の第 2 の実施の形態における複製端末発見方法の複製端末発見フェーズ（フェーズ # 1）の流れ

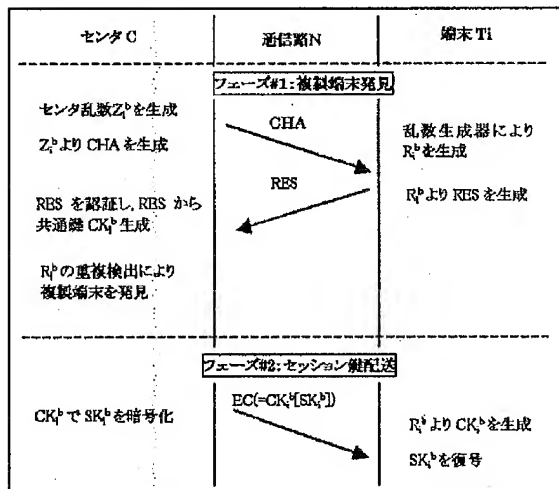
図、

【図 8】 本発明の第 2 の実施の形態における複製端末発見方法のグループ鍵配送フェーズ（フェーズ # 2）の流れ図である。

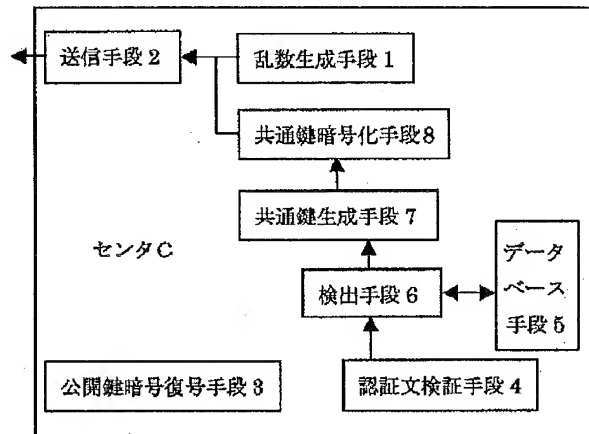
【符号の説明】

- 1 乱数生成手段
- 2 送信手段
- 3 公開鍵暗号復号手段
- 4 認証文検証手段
- 5 データベース手段
- 6 検出手段
- 7 共通鍵生成手段
- 8 共通鍵暗号化手段
- 9 共通鍵暗号復号手段
- 10 認証文生成手段
- 11 公開鍵暗号化手段

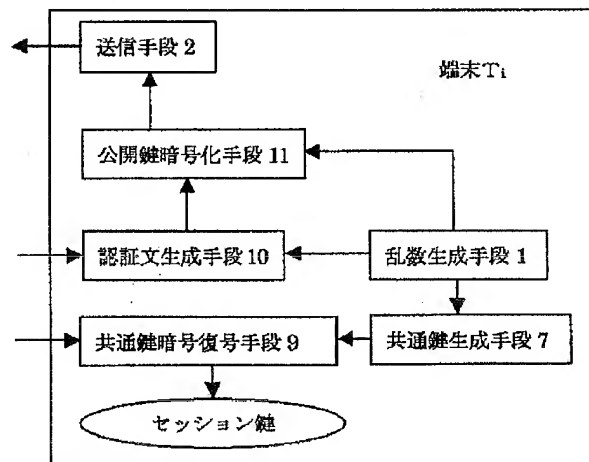
【図 1】



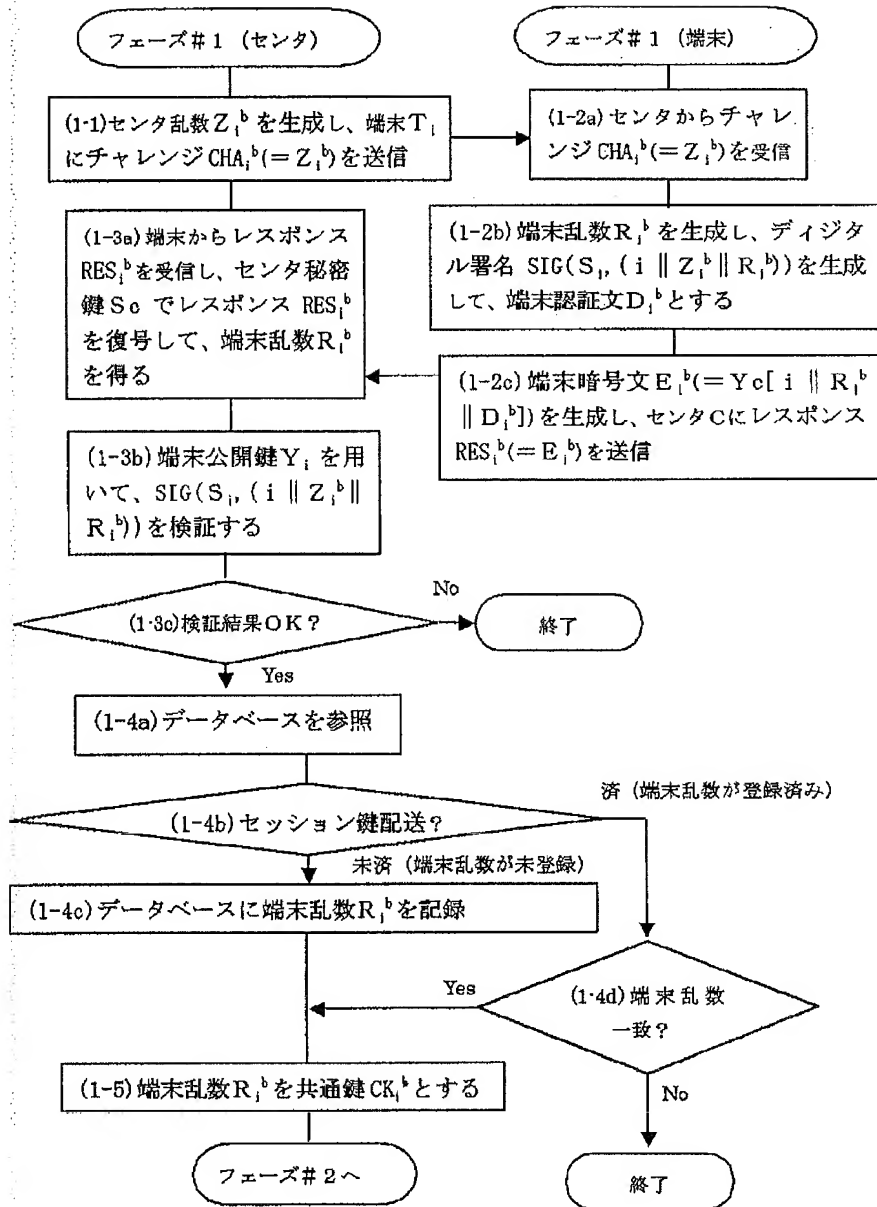
【図 2】



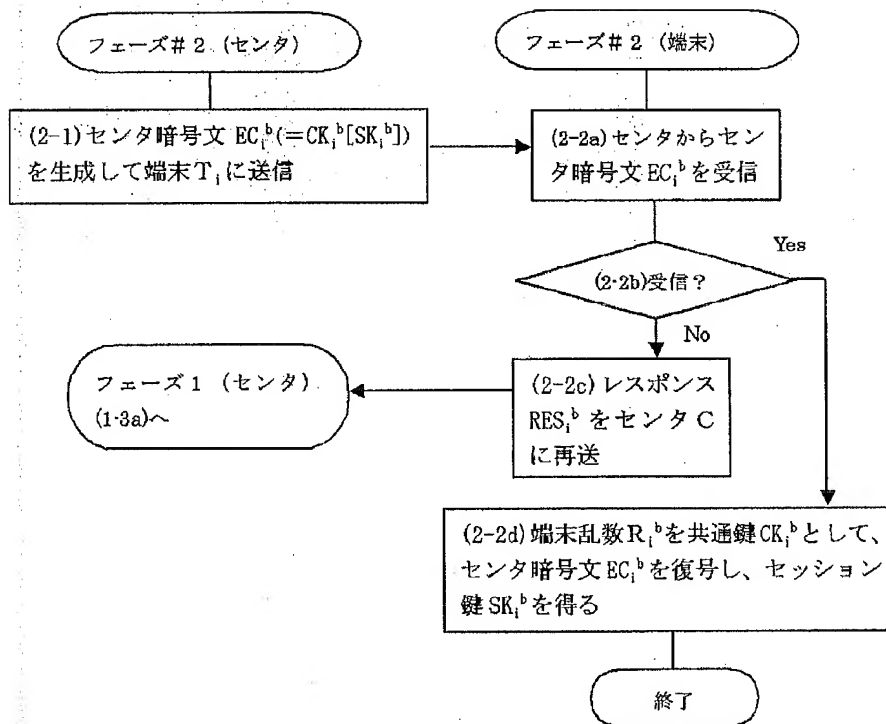
【図 3】



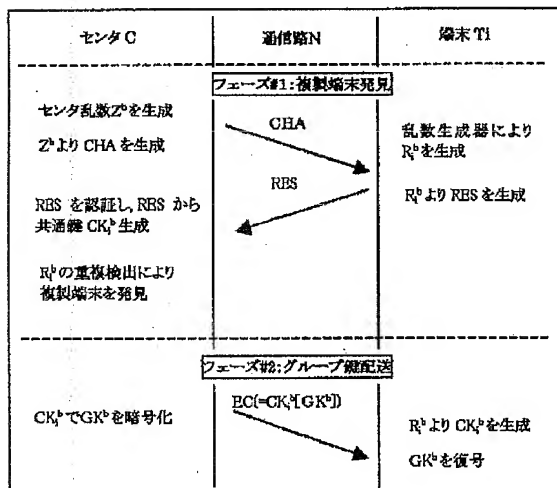
【図4】



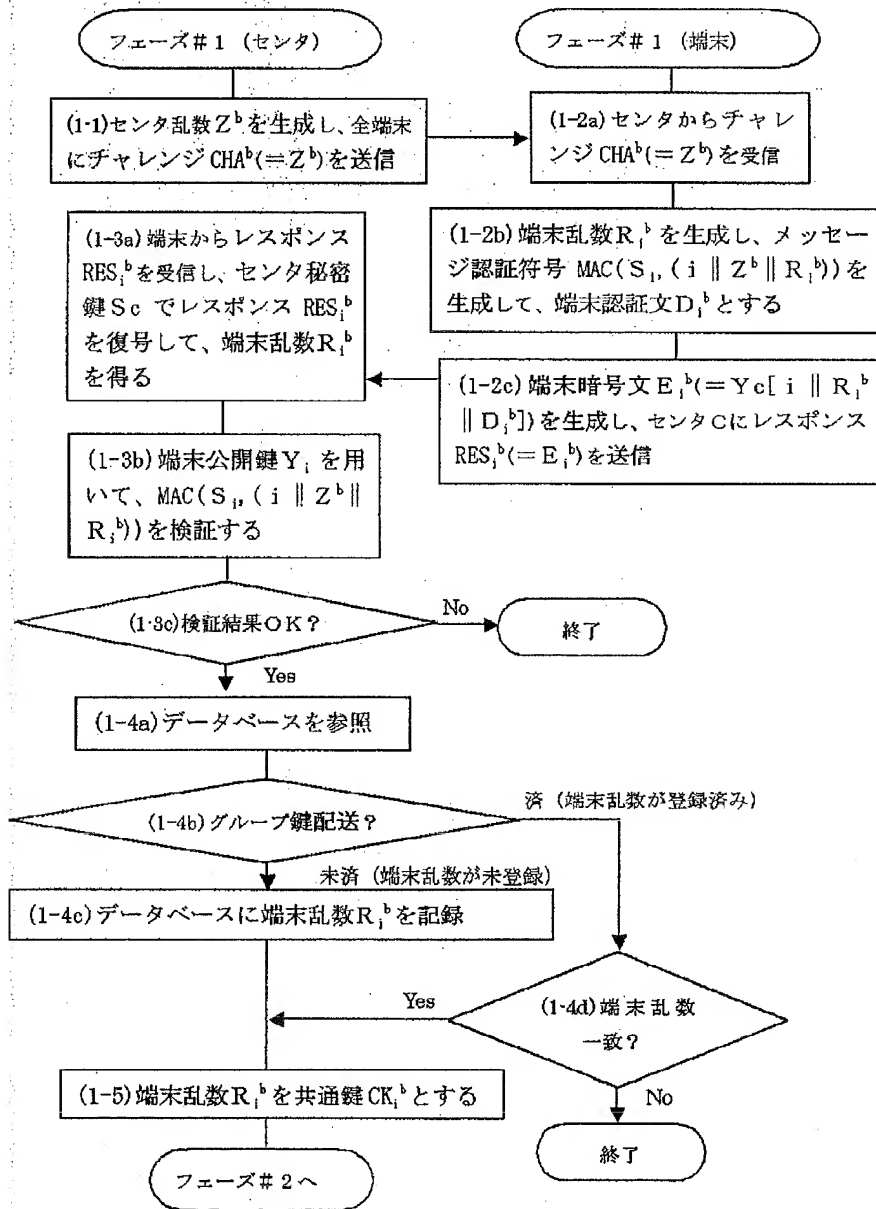
【図5】



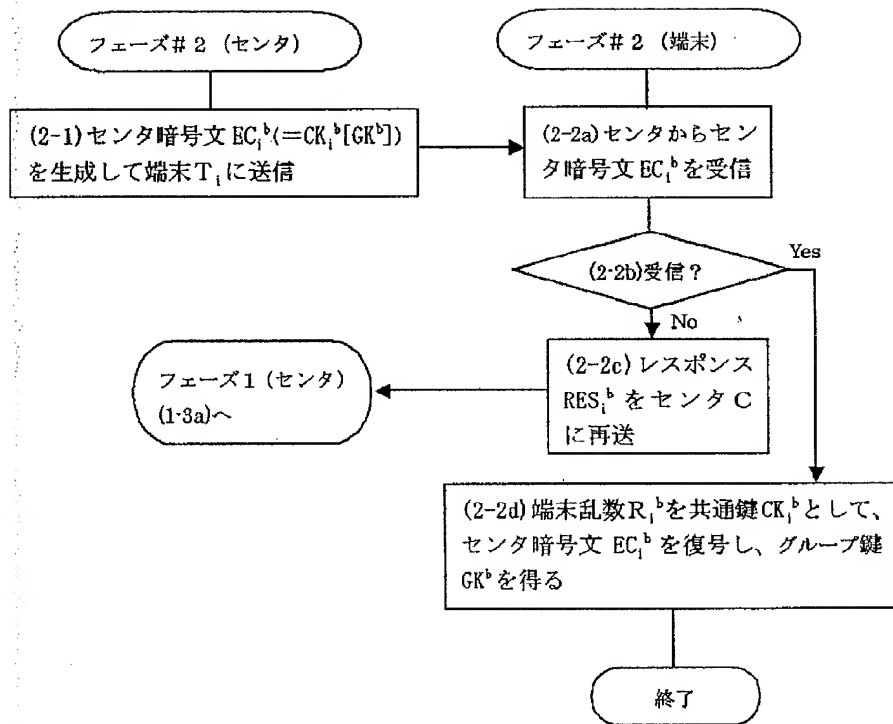
【図6】



【図7】



【図8】



フロントページの続き

(72)発明者 松崎 なつめ
 神奈川県横浜市港北区新横浜三丁目20番8
 号 株式会社高度移動通信セキュリティ技
 術研究所内
 (72)発明者 松本 勉
 神奈川県横浜市青葉区柿の木台13-45

Fターム(参考) 5B017 AA03 BA07
 5B085 AE29
 5J104 AA07 AA08 AA09 AA16 AA18
 BA03 EA06 EA18 KA02 KA06
 LA01 LA06 NA02 NA03